

RECEIVED
CENTRAL FAX CENTER
MAR 14 2011

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1-17 (Cancelled)

18. (Currently Amended) A system comprising:

a network interface to couple with a public network to receive a first client message and first data that is encrypted according to a wireless security format and to receive a second client message and second data that is encrypted according to a wired security format, wherein the network interface comprises a first port to receive the first client message and the first data, and wherein the first port has a number selected from a group consisting of numbers 9208 through 9282;

a selection system coupled with the network interface to select a first security format conversion for the first data and to select a second security format conversion for the second data; and

a conversion system coupled with the selection system to perform the first security format conversion on the first wireless security format encrypted data and to perform the second security format conversion on the second wired security format encrypted data based on a conversion indication received from the network interface including information regarding a type of conversion to implement.

19. (Currently Amended) The system of claim 18, wherein the network interface comprises ~~a first port to receive the first client message and the first data~~ and a second port to receive the second client message and the second data.

20. (Currently Amended) The system of claim 19, ~~wherein the first port has a number selected from the group consisting of the numbers 9208 through 9282, and~~ wherein the second port has number 443.

21. (Previously Presented) The system of claim 20, wherein the first port has the number 9208.

22. (Previously Presented) The system of claim 18, wherein the first data comprises Wireless Transport Layer Security encrypted data, and wherein the second data comprises Secure Sockets Layer encrypted data.

23. (Previously Presented) The system of claim 18, wherein the conversion system comprises a first security format conversion from the wireless security format encrypted data to plain data and a second security format conversion from the wired security format encrypted data to plain data.

24. (Previously Presented) The system of claim 18, wherein the selection system comprises:

logic to receive an indication of one of a plurality of ports of the network interface on which a client message was received from the public network; and

logic to select a security format conversion from among a plurality of format conversions including a first security format conversion from a Wireless Transport Layer Security format to another format and a second security format conversion from a Secure Sockets Layer format to another format in dependence upon the received indication of the port.

25. (Previously Presented) The system of claim 24, wherein the selection system further comprises:

logic to receive information about a security feature supported by a client access device, and wherein the logic to select the security format conversion is capable of selecting one of the plurality of format conversions in dependence upon the received indication of the port and the received information about the security feature supported by the client access device.

26. (Previously Presented) The system of claim 18, wherein the network interface, the selection system, and the conversion system are contained within a single network device.

27. (Previously Presented) The system of claim 26, residing in a data center between the Internet and a data center server.

28. (Previously Presented) The system of claim 26, residing in a data center between a first switch within the data center and a second switch within the data center.

29. (Currently Amended) A method comprising:

listening on a network interface for a first client message and first data that is encrypted according to a security format for wireless data and listening on the network interface for a second client message and second data that is encrypted according to a security format for wired data, wherein the listening includes listening on a first port that has a number selected from a group consisting of numbers 9208 through 9282 for the first client message and the first data;

receiving the first client message and the second client message from the network interface;

selecting a first security format conversion for the first data and selecting a second security format conversion for the second data; and

performing the first security format conversion on the first data and performing the second security format conversion on the second data based on a conversion indication received from the network interface.

30. (Currently Amended) The method of claim 29, wherein said listening on the network interface comprises listening ~~on a first port having a number selected from the group consisting of the numbers 9208 through 9282 for the first client message, and listening on the~~ on a second port having the number 443 for the second client message.

31. (Previously Presented) The method of claim 29, wherein said selecting comprises selecting a security format conversion from Wireless Transport Layer Security format to another format for the first data and selecting a security format conversion from Secure Sockets Layer format to another format for the second data.

32. (Previously Presented) The method of claim 31, wherein the other formats comprise plain data.

33. (Previously Presented) The method of claim 29:

wherein said listening, receiving, selecting, and performing, are each performed within a single network device; and

wherein the single network device resides within a data center disposed between the Internet and a data center server.

34. (Previously Presented) The method of claim 29:

wherein said listening, receiving, selecting, and performing, are each performed within a single network device; and

wherein the single network device resides within a data center and is disposed between a first data center switch and a second data center switch.

35. (Previously Presented) The method of claim 29, wherein at least a portion of said selecting or said performing is executed in hardware.

36. (Currently Amended) A machine-readable medium having stored thereon data representing sequences of instructions that if executed cause a machine to perform operations comprising:

listening on a network interface for a first client message and first data that is encrypted according to a security format for wireless data and listening on a second port of the network interface for a second client message and second data that is encrypted according to a security format for wired data, wherein the second port has a number 443;

receiving the first client message and the second client message from the network interface; and

selecting a first security format conversion for the first data and selecting a second security format conversion for the second data wherein the conversions are based on a conversion indication received from the network interface.

37. (Currently Amended) The machine-readable medium of claim 36, wherein the instructions that if executed cause the machine to listen further comprise instructions that if executed cause the machine to listen on a first port having a number selected from the group consisting of the numbers 9208 through 9282 for the first client message, ~~and listening on the second port having the number 443 for the second client message.~~

38. (Previously Presented) The machine-readable medium of claim 36, wherein the instructions that if executed cause the machine to select further comprise instructions that

if executed cause the machine to select a security format conversion from Wireless Transport Layer Security format to another format for the first data and select a security format conversion from Secure Sockets Layer format to another format for the second data.

39. (Previously Presented) The machine-readable medium of claim 38, wherein the other formats comprise plain data.

40. (Currently Amended) A method comprising:

receiving an indication of one of a plurality of ports on which a client message was received from a public network including information regarding a type of conversion to implement, wherein the plurality of ports comprise a first port having a number selected from numbers 9208 through 9282; and

selecting a security format conversion from among a plurality of format conversions including a first security format conversion from a Wireless Transport Layer Security format to another format and a second security format conversion from a Secure Sockets Layer security format to another format based upon the received indication from the port.

41. (Currently Amended) The method of claim 40, wherein the plurality of ports comprise ~~a first port having a number selected from the group consisting of the numbers 9208 through 9282 and~~ a second port having number 443.

42. (Previously Presented) The method of claim 40, wherein the other formats comprise plain data formats.

43. (Previously Presented) The system of claim 23, further comprising a second network interface to provide the plain data.

44. (Previously Presented) The method of claim 32, further comprising providing the plain data from a second network interface.

45. (Previously Presented) The machine-readable medium of claim 39, wherein the instructions further comprise instructions that if executed cause the machine to provide the plain data from a second network interface.

46. (Previously Presented) The method of claim 40, further comprising:

performing the selected security format conversion to plain data; and

providing the plain data to a network through a network interface.

47. (Currently Amended) A system comprising:

a first network interface within a data center to couple with a public network to receive a first Wireless Transport Layer Security encrypted data from a cell phone client on a port with a number in a range of 9208 through 9282, and to receive a second Secure Sockets Layer encrypted data from a personal computer client;

a conversion system within the data center to convert the first Wireless Transport Layer Security encrypted data received from the cell phone client to plain data and to convert the second Secure Sockets Layer encrypted data received from the personal computer client to plain data based on a conversion indication received from the network interface;

a second network interface within the data center and couplable with a private network to provide the plain data to the private network.

48. (Previously Presented) The system of claim 47, wherein the first and second network interfaces are logically disposed between first and second switches in the data center.